UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/514,978	02/29/2000	Mary Ellen Zurko	C99020US	2130

22879 7590 06/14/2004

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
DARROW, JUSTIN T	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/14/2004

11

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/514,978	Applicant(s) ZURKO ET AL.
	Examiner Justin T. Darrow	Art Unit 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 April 2000*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-29 and 32-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *38-41* is/are allowed.

6)☒ Claim(s) *21-29 and 32-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *9*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-41 have been presented for examination. Claims 1-20 have been canceled in a preliminary amendment filed 02/29/2000. Claims 24, 29, and 32 have been amended and claims 30 and 31 have been canceled in an amendment filed 04/22/2004. Claims 21-29 and 32-41 have been examined.

Priority

2. Acknowledgment is made that the instant application is a division of Application No. 07/479,666, filed 02/13/1990, now U.S. Patent No. 6,507,909 B1.

Drawings

3. The drawings were received on 04/22/2004. These drawings are approved.

Response to Arguments

4. Applicant's arguments filed 04/22/2004 have been fully considered but they are not persuasive.

5. As per claims 29-32, the applicant's assertion that detecting a trusted shell environment is not equivalent to verifying the trusted command is erroneous. Interpreting an asserted claim should first consider intrinsic evidence such as the claims themselves and the specification. See *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582, 39 USPQ2d 1573, 1576 (Fed. Cir. 1996). The specification describes verifying the trusted command (see page 20, lines 6-14; figure 2, items 10 and 14; submitting a parsed representation of the trusted command by making

a kernel call where the nature of the kernel call is recognized). Johri et al., U.S. Patent No. 4,918,653 A teaches verifying the trusted command in the trusted mode (see column 22, lines 53-55; detecting the trusted shell by reading the corresponding /etc/utmp entry; see column 22, lines 23-28; where finding the type of that running process by reading the ut_type field which is either USER_PROCESS, if the trusted path was not created, or TSH_PROCESS, if the trusted shell was created) after communicating a representation of the trusted command in the trusted mode (see column 22, lines 16-23; sending a SIGSAK signal to all the processes to terminate then fork trusted child processes).

6. As per claims 32-37, Johri et al. does disclose issuing a message to indicate a transition to the untrusted mode (see column 22, lines 47-49; if the user presses the SAK again while in the trusted shell, the same set of operations are performed as when the user logged in; see column 22, lines 17-19; the line discipline driver sends the SIGSAK signal to all the processes) before transitioning from the trusted mode to the untrusted mode (see column 22, lines 50-55; the current trusted shell is terminated and the user exits the trusted shell; see column 26, lines 2-12; figure 8, State S1; before login in the untrusted shell in State 1, pressing the Secure Attention Key immediately comes back to State 1).

7. As per claims 21-28, in response to applicant's argument that Rivest et al., U.S. Patent No. 4,405,829 A is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). Additionally, "a reference is reasonably pertinent if, even though it may be in a different field

from that of the inventor's endeavor, it is one which, because of the matter with which it deals, logically would have commended itself to an inventor's attention in considering his problem." *In re Clay*, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992). Any specific hint or suggestion in a particular reference to support the combination of the references is required to resolve a factual question of motivation to determine a legal conclusion of obviousness. See *In re Lee*, 61 USPQ2d 1430, 1434 (Fed. Cir. 2002). The motivation to combine two references may be found in the text of both references. See *In re Thrift*, 63 USPQ2d 2002, 2007 (Fed. Cir. 2002). In this case, Johri et al. describes a login program in an untrusted environment that authenticates a user by encrypting a user-entered password and comparing the encrypted user-entered password with an encrypted list of passwords (see column 26, lines 52-58). Because the untrusted environment of the login program is publicly accessible by other users (see Johri et al., column 19, lines 48-52; multi-user operating system; see Johri et al., column 22, lines 1-4; where access is available by programs in an untrusted state), there is motivation to have a public file with an enciphering key, with a separate corresponding deciphering key (see Rivest et al., column 2, lines 43-50). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method of Johri et al. with the parsing of Rivest et al. to have a public key stored in an untrusted environment for encrypting a password to be compared with a list of encrypted passwords that cannot be decrypted by the public key by other users (see Johri et al., column 26, lines 43-51).

Additionally, the applicant's argument that a public key algorithm is contrary to the subject invention is also incorrect. The invention checks the parsed command for correctness (see specification, page 15, lines 4-6). Public key algorithms are customarily used to determine

data correctness and integrity (see Rivest et al., column 3, lines 9-22; a recipient, who knows the content of a message, determining a change in the substance of the message with a message-dependent digital signature).

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 29 and 32-37 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 32 recites the limitation "the communication step" in line 5. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting "verifying the trusted command in the trusted mode after the communication step; and communicating a representation of the trusted command in the trusted mode." in lines 4-6 and replacing with --communicating a representation of the trusted command in the trusted mode; and verifying the trusted command in the trusted mode after the communicating step.--.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

11. Claims 29 and 32-37 are rejected under 35 U.S.C. 102(e) as being anticipated by Johri et al., U.S. Patent No. 4,918,653 A.

As per claim 29, Johri et al. describe a method of processing a trusted command comprising:

interpreting a trusted command in an untrusted mode (see column 27, lines 3-6; figure 13; pressing the Secure Attention Key to be interpreted in the untrusted mode; see column 22, lines 16-20; causing the line discipline driver to send a SIGSAK signal to all processes within the untrusted mode running on the terminal to terminate);

executing the trusted command in a trusted mode (see column 22, lines 25-38; forking a new child process to create a trusted shell then creating a trusted path for the user's terminal and protecting the terminal from reading and writing by unauthorized programs);

communicating a representation of the trusted command in the trusted mode (see column 22, lines 16-23; sending a SIGSAK signal to all the processes to terminate then fork trusted child processes); and

verifying the trusted command in the trusted mode after the communication step (see column 22, lines 53-55; detecting the trusted shell by reading the corresponding /etc/utmp entry; see column 22, lines 23-28; where finding the type of that running process by reading the ut_type field which is either USER_PROCESS, if the trusted path was not created, or TSH_PROCESS, if the trusted shell was created).

As per claim 32, Johri et al. moreover point out:

requesting confirmation of the trusted command in the trusted mode (see column 22, lines 53-55; when the user requests to exit the trusted shell).

As per claim 33, Johri et al. also specifies:

using the trusted command in the untrusted mode (see column 22, lines 16-20; sending the SIGSAK signal to all processes within the controlling terminal process group in the untrusted shell to terminate the user processes).

As per claim 34, Johri et al. next delineate:

transitioning from the untrusted mode to the trusted mode (see column 22, lines 23-38; if the trusted path is not created, creating the trusted path; see column 27, lines 3-8; figure 13; terminating the untrusted shell and creating in its place the trusted shell).

As per claim 35, Johri et al. alternatively discuss:

transitioning from the trusted mode to the untrusted mode (see column 22, lines 50-55; the current trusted shell is terminated and the user exits the trusted shell; see column 26, lines 2-12; figure 8, State S1; before login in the untrusted shell in State 1, pressing the Secure Attention Key immediately comes back to State 1).

As per claim 36, Johri et al. further elaborate that:

issuing a message to indicate a transition to the untrusted mode before the transitioning step (see column 22, lines 47-49; if the user presses the SAK again while in the trusted shell, the same set of operations are performed as when the user logged in; see column 22, lines 17-19; the line discipline driver sends the SIGSAK signal to all the processes).

As per claim 37, Johri et al. subsequently describe:

detecting if a command is a trusted command in an untrusted mode (see column 26, lines 9-23; figure 8, States S1, S2, and S3; carrying out the command of pressing the Secure Attention Key if the user has successfully logged in).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 21-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Johri et al. U.S. Patent No. 4,918,653 A in view of Rivest et al., U.S. Patent No. 4,405,829 A.

As per claim 21, Johri et al. illustrates a computing environment to process a trusted command, comprising:

an untrusted environment to encrypt a trusted command to be compared with encrypted passwords on a list (see column 26, lines 2-7 and 15-17; figure 8, States 1 and 2; State 1 is before login and State 2 is the state after login in an untrusted shell, but before the trusted shell; see column 26, lines 48-61; figure 11; the login program encrypts the password entered by the user as a command to login); and

a trusted environment to receive the trusted command from the untrusted environment (see column 27, lines 33-36; figure 14; typing the password command where the password command is in the trusted shell) and to communicate a representation of the trusted command (see column 27, lines 41-44; figure 14; having that command execute and then returning to the trusted shell).

Although Johri et al. disclose encrypting a trusted command (see column 26, lines 48-61; figure 11; the login program encrypts the password entered by the user as a command to login), they do not explicitly teach parsing a trusted command.

Rivest et al. describe encrypting a message by parsing (see column 4, lines 32-37; breaking the message into message block words before encoding).

Because the untrusted environment of the login program is publicly accessible by other users (see Johri et al., column 19, lines 48-52; multi-user operating system; see Johri et al., column 22, lines 1-4; where access is available by programs in an untrusted state), there is motivation to have a public file with an enciphering key, with a separate corresponding deciphering key (see Rivest et al., column 2, lines 43-50). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method of Johri et al. with the parsing of Rivest et al. to have a public key stored in an untrusted environment for encrypting a password to be compared with a list of encrypted passwords that cannot be decrypted by the public key by other users (see Johri et al., column 26, lines 43-51).

As per claim 22, Johri et al. further point out:

that the trusted environment executes the trusted command (see column 27, lines 33-39; figure 14; the first transition in the trusted shell involves the execution of the password command) if the trusted environment detects confirmation of the trusted command (see column 26, lines 11-25; figure 8; where the trusted shell is available only after a successful login with the correct password).

As per claim 23, Johri et al. also describe:

the representation of the trusted command is communicated through a trusted path (see column 27, lines 41-44; figure 14; returning the command to the trusted shell; see column 27,

lines 21-28; figure 13; establishing the trusted path; see column 27; lines 9-12; figure 13; between the user and the trusted shell);

As per claim 24, Johri et al. additionally specify:

that the trusted path is between the user and the trust environment (see column 27, lines 9-12; figure 13; the trusted path between the user and the trusted shell).

As per claim 25, Johri et al. then mention:

a user interface to communicate with the untrusted environment (see column 26, lines 48-52; figure 11; a terminal for the user to login to the untrusted shell) and the trusted environment (see column 26, lines 3-7; figure 8; user is actually in the trusted shell).

As per claim 26, Johri et al. depict a method of processing a trusted command, comprising:

encrypting a trusted command to be compared with encrypted passwords on a list, in an untrusted mode of a system (see column 26, lines 2-7 and 15-17; figure 8, States 1 and 2; State 1 is before login and State 2 is the state after login in an untrusted shell, but before the trusted shell; see column 26, lines 48-61; figure 11; the login program encrypts the password entered by the user as a command to login);

establishing a trusted mode of the system (see column 26, lines 3-7; figure 8, State 3; the user going into the trusted shell); and

communicating a representation of the trusted command in the trusted mode (see column 27, lines 41-44; figure 14; having the password command execute and then returning to the trusted shell).

Although Johri et al. disclose encrypting a trusted command (see column 26, lines 48-61; figure 11; the login program encrypts the password entered by the user as a command to login), they do not explicitly teach parsing a trusted command.

Rivest et al. describe encrypting a message by parsing (see column 4, lines 32-37; breaking the message into message block words before encoding).

Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method of Johri et al. with the parsing of Rivest et al. to have a public key stored in an untrusted environment for encrypting a password to be compared with a list of encrypted passwords that cannot be decrypted by the public key (see column 26, lines 43-51).

As per claim 27, Johri et al. further point out:

executing the trusted command in the trusted mode (see column 27, lines 33-39; figure 14; the first transition in the trusted shell involves the execution of the password command) if confirmation of the trusted command is detected (see column 26, lines 11-25; figure 8; where the trusted shell is available only after a successful login with the correct password).

As per claim 28, Johri et al. next discuss:

displaying a representation of the trusted command (see column 5, lines 22-26; figure 1; a display for characters sent to the display device; see column 27, lines 41-44; issuing the password command resulting in the changed password displayed to the user).

Allowable Subject Matter

14. Claims 38-41 are allowed.

15. The following is an examiner's statement of reasons for allowance:

Claims 38-41 are drawn to method for executing a trusted command. The closest prior art, Johri et al. U.S. Patent No. 4,918,653 A in view of Rivest et al., U.S. Patent No. 4,405,829 A, disclose a similar method. Johri et al. describes encrypting a trusted command to be compared with encrypted passwords on a list, in an untrusted mode of a system (see column 26, lines 2-7 and 15-17; figure 8, States 1 and 2; State 1 is before login and State 2 is the state after login in an untrusted shell, but before the trusted shell; see column 26, lines 48-61; figure 11; the login program encrypts the password entered by the user as a command to login). Rivest et al. specify encrypting a message by parsing (see column 4, lines 32-37; breaking the message into message block words before encoding). However, they teach away from submitting the parsed command to the trusted computing environment; and performing a security check on the parsed command and user identification data in the trusted computing environment. This composite recitation explicitly incorporated into independent claim 38 renders claims 38-41 allowable.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue

fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

16. Applicant's amendment necessitated the new grounds of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (703) 305-3872 and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (703) 305-1830.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.

June 8, 2004

Justin Darrow

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100